What is claimed is:

[Claim 1] A method comprising:

separating a random number generator into a first stage and second stage;
replicating the circuitry of said second stage into M parallel modules; and
generating M random number outputs using a single first stage circuitry and M parallel second stage modules.

[Claim 2]

A method according to claim 1 wherein each of said M modules have a first input which is the output result of said single first stage circuitry and second input, which is the unique to the module.

[Claim 3]

A method according to claim 2 wherein said first stage circuitry has at least two first stage inputs, a first first stage input representing the integer coordinate components of the location of interest and a second first stage input representing the hardware cycle.

[Claim 4]

A method according to claim 3 wherein generating includes:
storing said first stage inputs in a first register;
selecting a first set of bits from said first register;
storing said first set of bits in a second register; and
selecting a second set of bits from said second register, said second set of bits representing said result of said single first stage circuitry.

[Claim 5]

A method according to claim 4 wherein for each parallel second stage module, generating further includes:
storing said result of said single stage circuitry in a second stage register; and
selecting a second set of bits from said second stage register, said second set of bits representing one of said M random number outputs.

[Claim 6]

A method according to claim 5 wherein said each random number output can be one of a phase 1 output and a phase 2 output.

[Claim 7]

A method according to claim 6 wherein said phase 2 output is a full and exact representation of the desired random number output.

[Claim 8]

A method according to claim 7 wherein said phase 1 output is an approximation of said phase 2 output.

[Claim 9]

A method according to claim 4 wherein selecting said first set of bits includes:
utilizing a group of XORs, each XOR having its inputs pre-wired to various locations of said first register, to select among the bits of said inputs.

[Claim 10]

A method according to claim 4 wherein selecting said second set of bits includes:
utilizing a group of XORs, each XOR having its inputs pre-wired to various locations of said second register, to select among the bits stored therein.

[Claim 11]

A method according to claim 5 wherein said selecting in each parallel second stage module includes:
utilizing a group of XORs, each XOR having its inputs wired to a number of bits representing the module number and to selected locations of said second stage register.

[Claim 12]

A method according to claim 11 wherein the wired number of bits representing the module number varies from XOR to XOR.

[Claim 13] A method according to claim 11 wherein each parallel second stage module wires its XORs to its registers in an identical manner with all other parallel second stage modules.

[Claim 14] An apparatus configured to generate M random number outputs on a given cycle j in a parallel fashion, comprising:

a first stage circuitry configured to accept a series of inputs; and
M second stage modules, the output of said first stage wired as an input each of said M modules, the output of each module one of said M random number outputs.

[Claim 15]

An apparatus according to claim 14 wherein said series of inputs includes the cycle number j, the number of dimensions desired and integer coordinate components for each dimension desired.

[Claim 16]

An apparatus according to claim 14 wherein each said second stage module also includes an input k representing the number of the module.

[Claim 17]

An apparatus according to claim 15 each said random number output contains a fractional coordinate component for each desired dimension as well as a weight of the

corresponding pulse at the location given said fractional coordinate components and said integer coordinate components.

[Claim 18]

An apparatus according to claim 14 wherein said first stage circuitry comprises:
a first register having locations storing each bit of said series of inputs; and
a first bank of XORs, each input of each said XOR of said first bank coupled to an arbitrary one of said locations of said first register.

[Claim 19]

An apparatus according to claim 18 wherein said first stage circuitry further comprises:
a second register having locations storing each output of said first bank of XORs; and
a second bank of XORs, each input of said XORs of said second bank coupled to an arbitrary one of said locations of said second register, each output of said second bank of XORs representing each bit of said output of said second stage.

[Claim 20]

An apparatus according to claim 16 wherein each second stage module comprises:
a first register having locations configured to store each bit of said output of said first stage; and
a bank of XORs having one set of inputs from said first register and a second set of inputs from the bits of input k, the output of each XOR representing one bit of said random number output.

[Claim 21]

An apparatus according to claim 20 wherein said M second stage modules produce an approximation of the full said random number output.